1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 2013

(b) Name of system: Public Affairs Web Services

(c) System acronym: PAWS

(d) IT Asset Baseline (ITAB) number: 1077

(e) System description (Briefly describe scope, purpose, and major functions):

Public Affairs Web Services (PAWS) aids PA in carrying out the Secretary's mandate to help Americans understand the importance of foreign affairs**.** PAWS arranges contacts with Department officials and private citizens and groups through Washington conferences, briefings, and seminars, and through regional town hall meetings and media engagements across the country.

PAWS requires a number of applications to disseminate information used in daily briefings, television programs, and support of the state.gov website. Moreover, the information is 100% unclassified and provides users with discretionary access to materials needed to conduct the Bureau's mission.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): None

(h) Date of previous PIA (if applicable): Unknown

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The records of PAWS contain: Name, job title, gender, business addresses, organizations, business telephone, fax number, and business email addresses of media representatives (anyone who works for a newspaper, magazine, radio or television station, wire service, or any other form of media) who request interviews with the Secretary of State and Department Principals or have been contacted for media events, interviews, occasions, invitations, travel opportunities or placement of articles. Records in PAWS are obtained directly from the individual who is the subject of these records or the agency or organization that the individual represents.

b. How is the information collected?

Information is collected through an internal website that contains links to obtain the data and web-based applications needed for content management that are only available/function on the PA system. Information is obtained:

- By phone conversation where a potential contact relays his/her information to a PA representative. The information is entered into Touch Base- a database in PAWS which includes Press Guidance, Idea Scale, USDC, and PANews- run by PA to collect information on events, press briefings, and other State engagements, and
- Via a public-facing webpage allowing contacts to register for Bureau mailing lists, notifications and updates (https://public.govdelivery.com/accounts/USSTATEBPA/subscriber/new?).

This application is hosted in a server farm by the Bureau of Information Resource Management (IRM) at the Department of State. However, PA is the sole administrator of the data and the web applications.

c. Why is the information collected and maintained?

The information collected in PAWS is used by PA at the Department of State to arrange contacts between Department officials and private citizens and groups, organize office data, and keep track of the information dissemination from the office to the worldwide public or other offices. Accordingly, soliciting this information allows the Department of State's Bureau of Public Affairs to establish and maintain contact with members of civil society organizations, by targeting individuals based on self-identified regional and policy interests. The Bureau of Public Affairs is responsible for ensuring that members of the American public understand the importance of foreign affairs, which includes

various forms of public engagement, including conferences and briefings, email updates, conference calls, public forums, etc. More locally, the information in PAWS allows PA to track the activities of its office, as well as anyone who has requested access to media events.

d. How will the information be checked for accuracy?

These records contain information obtained directly from the individual who is the subject of these records, the agency or organization that the individual represents, published directories and/or other bureaus in the Department. Accordingly, information in PAWS is assumed to be reliable.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 5 U.S.C. 301 (Management of Department of State)
- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 U.S.C. 3921 (Management of the Foreign Service)
- Title 22 – Federal Regulations, Code of Federal Regulations; Title PART 9b – Regulations Governing Department of State Press Building Passes

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

PAWS collects the minimum amount of personally identifiable information necessary to perform its statutorily mandated functions. Information is hosted on PAWS, which has adequate management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the Information Assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The data in PAWS is used to disseminate information on domestic speaking engagements, press briefings, and conferences. Additionally, information is collected to allow people to receive invitations to attend events at the Department, email updates about major policy announcements and initiatives, a bi-weekly newsletter, and/or to be notified when the Department is participating in events in the registrant's city.

b. What types of methods are used to analyze the data? What new Information may be produced?

PAWS is only used to store information sets for the Department of State, and its data is not analyzed. No data mining is used to analyze the data contained in PAWS. Also, no new information is produced in this system.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

PAWS does not directly use any information from any third party commercial applications or any other Federal agency databases. PAWS is an unclassified repository used only by the Bureau of Public Affairs (PA).

d. Are contractors involved in the uses of the PII?

The system is government-owned and was primarily designed and developed by full-time equivalent (FTE) employees. However, contractors are used in the operation and maintenance of the system. All personnel are required to abide by regulatory guidelines and have signed and follow DS's Rules of Behavior.

All users, including personnel at USAID who will access the database through secure FOBs, are required to sign and abide by the Department of State's "Rules of Behavior," and undergo training specific to the Civilian Response Corps Database.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Adequate safeguards are in place to preserve data accuracy, confidentiality, availability and integrity, to avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risks. Strenuous security controls are in place to ensure the protection of the PII and negate the threat of function creep. No data mining is performed on the information in PAWS. In addition, access is controlled through the use of user

identification, password and role-based privileges within the system and requires the user to frequently change his/her password. When a staff member resigns his/her employment or is terminated, the permissions will be changed on the database folder so that he/she will no longer be able to access it.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's disposition schedule. Schedule A-22-003-10, Media Correspondents' Records, states that these records should be destroyed when no longer needed for operations. Schedule A-22-003-05, Press Materials from Secretary's Trips, states that this data should be saved in four-year blocks by administration and then retired to the Records Service Center for immediate transfer to the National Archives. Schedule A-22-004-07, Speaking Engagement Files, states that records should be destroyed two years after the speaking engagement. Schedule A-22-004-08, Speakers' Biographic Files, states that records should be retained until the officer has left the Government or is deceased.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The records disposition schedules are appropriate and flexible enough to reduce privacy risk. Records may be purged from the system when no longer in use or when their schedule dictates.

Access to computerized files is password-protected and under the direct supervision of the system manager.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information may be used to assist the U.S. Department of State in interagency planning and coordinating public engagement activities. Specifically, information regarding speaking engagements is shared with the Office of the Secretary through email correspondence.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information in PAWS will be transmitted interagency through secured State email addresses. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

When shared within the Department, all information is still used in accordance with departmental procedures. Risks to privacy are mitigated by granting access only to authorized persons.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Information contained in PAWS may be made available as a routine use to other government agencies such as the U.S. Agency for International Development (USAID) and the White House. Typically, this information concerns speaking engagements, travel schedules of the Secretary of State, or data on summits hosted by the Department of State.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information in PAWS will be transmitted intra-agency through secured State email addresses.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risk to external relationship is limited to coordination of media events; therefore privacy risk to external events is limited.

8. Notice

The system:

☒ contains information covered by the Privacy Act.
STATE-22, Records of the Bureau of Public Affairs
STATE-79, Digital Communication and Outreach

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?
Yes, notice of the purpose, use, and authority for collection of information submitted is described in the System of Records Notices titled STATE-22 and STATE-79. Additionally, a privacy notice is posted at the bottom of the website where users register to receive information about upcoming Department events or relevant news items on a certain topic concerning diplomacy (https://public.govdelivery.com/accounts/USSTATEBPA/subscriber/new?).

b. Do individuals have the opportunity and/or right to decline to provide information?
When registering on the above-mentioned website (https://public.govdelivery.com/accounts/USSTATEBPA/subscriber/new?), individuals will not be able to receive desired information if they do not submit their personal information. Notice of the purpose, use and authority for collection of this and any other information submitted to PAWS are also described in the System of Records Notices titled STATE-22 and STATE-79.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?
All information requested is necessary for its intended purpose. Individuals on the registration website (https://public.govdelivery.com/accounts/USSTATEBPA/subscriber/new?) who do not provide all required personal information will not be able to properly sign up for mailing lists and receive invitations to attend Department events.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.
Individuals are informed how their information will be used in the System of Records Notices titled STATE-22 and STATE-79. Additionally, a privacy notice on the registration website provides users with notice as to the collection of their PII.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals who do not have access to PAWS cannot access their information and, therefore, cannot request it to be changed if they believe it to be incorrect. However, the PII in PAWS is collected from the record subjects themselves over the phone or on the registration website, so they can ensure that their information is accurate by providing accurate information. If they incorrectly submitted information on the registration website, individuals can resubmit their registration.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

All records containing personal information are maintained in the department secure ESOC DMZ, access to which is limited to authorized personnel. Potential users of PAWS must contact the database administrator in PA/EX/IT to request access to the system. To login to PAWS, a user must obtain a username and password. Access to PAWS requires a username and password and is under the direct supervision of the system manager. To access the system, users must be authorized to log into the Department of State's unclassified network. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

During the certification and authorization (C&A) process for PAWS, IRM/IA examined organizational records or documents and determined that PAWS, in accordance with access control policy and procedures: (i) enforces the maximum number of consecutive invalid access attempts within a certain period of time; (ii) automatically enforces a limit

of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period; and (iii) enforces automatic locks on the account/node for an organization-defined time period or delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to take the course entitled Protecting Personally Identifiable Information (PA-459) and information system security awareness training, including the procedures for handling Sensitive but Unclassified (SBU) information and personally identifiable information. Annual refresher training is mandatory. Before being granted access to PAWS, a user must first be granted access to the Department of State unclassified network.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to access to information in PAWS. PA/EX/IT database administrators have the discretion to grant or deny access to users in PAWS. Access is granted based solely on the identity of those users who have been approved to access the information. Furthermore access control lists define who can access the information and at what privilege level, and are regularly reviewed; inactive accounts are promptly terminated. Contractors who support PAWS are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain U.S. Government agencies (e.g., criminal law enforcement and Homeland Security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual.

11. Technologies

a. What technologies are used in the systems that involve privacy risk?

All hardware, software, and databases are vulnerable to risk, though no technology is used in PAWS that presents a greater privacy risk than normal.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No uncommon technologies exist in PAWS that would elevate its privacy risk.

12. Security

What is the security certification and accreditation (C&A) status of the system?

PAWS has received a full 36 month Authorization to Operate (ATO), which expires January 2014.